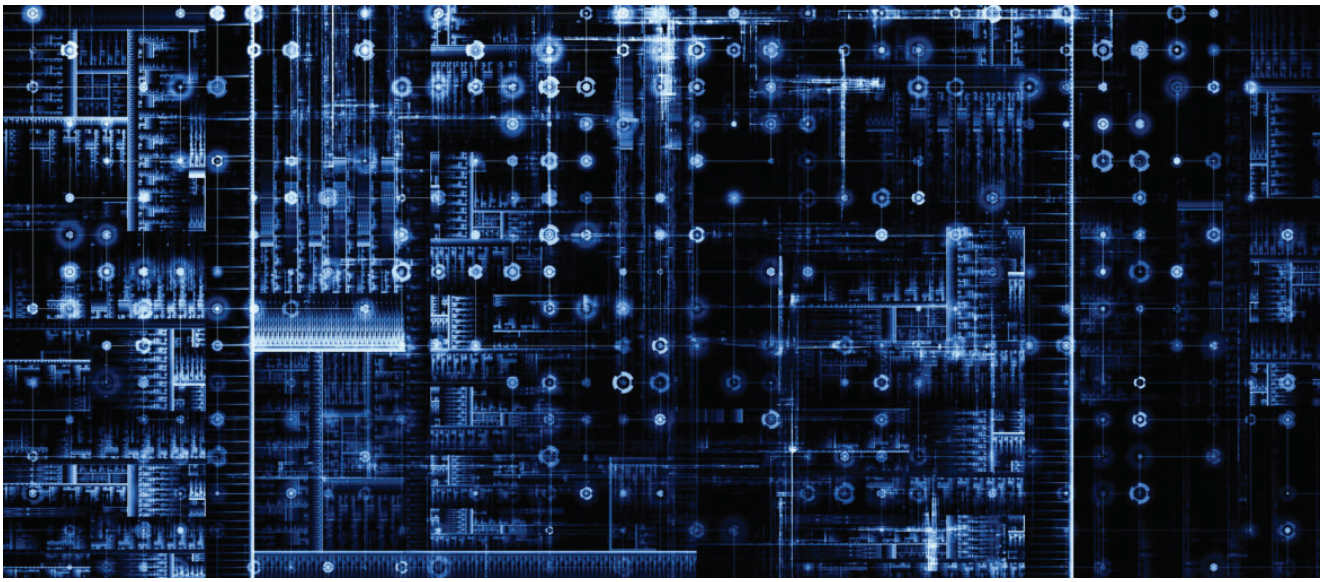
Exhibit E

Hackers Are Stealing More Cryptocurrency From DeFi Platforms Than Ever Before

blog.chainalysis.com/reports/2022-defi-hacks

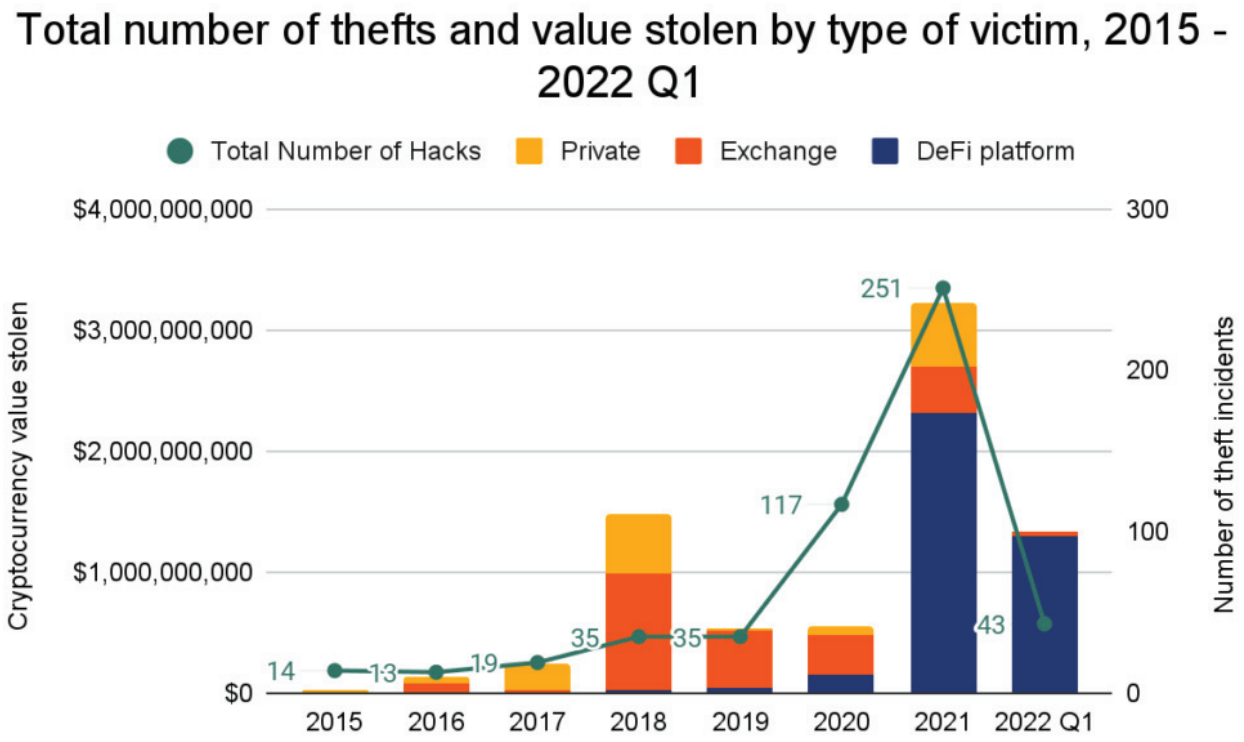
April 14, 2022



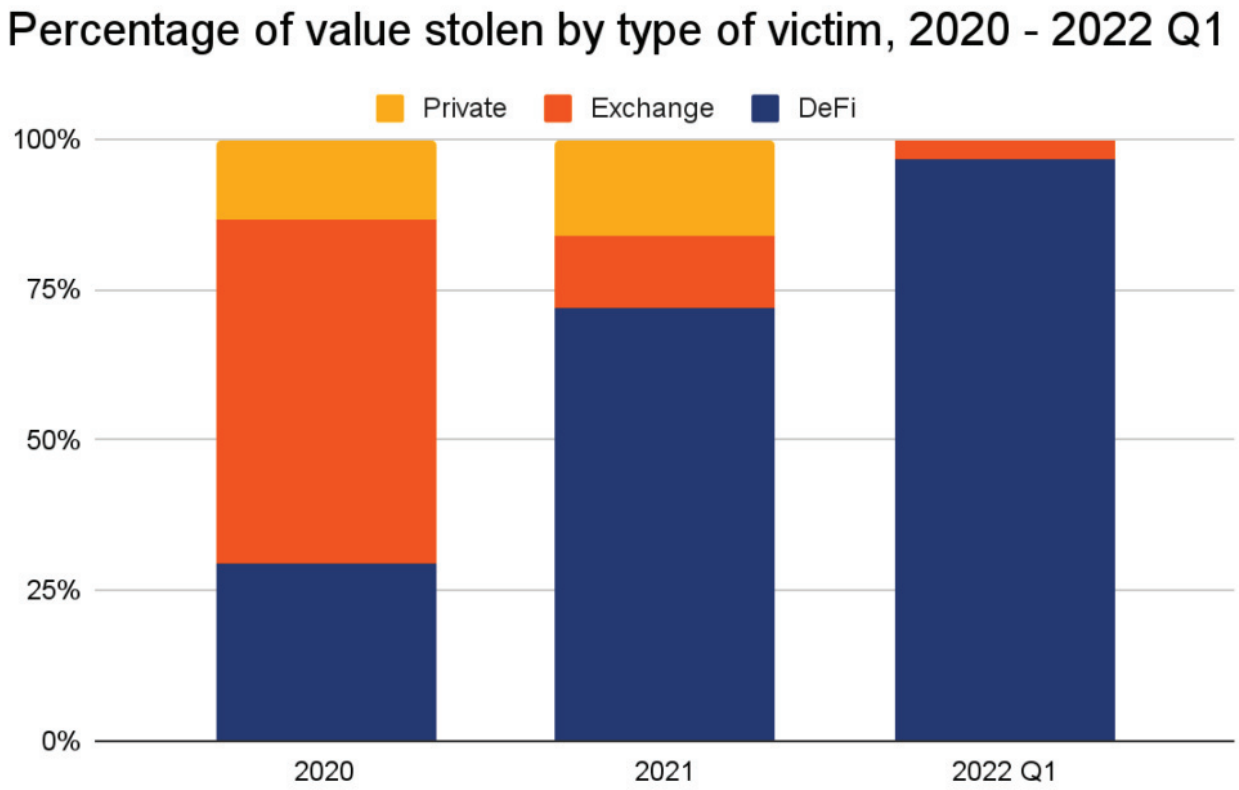
This blog builds on research featured in the 2022 Crypto Crime Report. Download your copy today.

Digital thieves had a big year in 2021, stealing $3.2 billion worth of cryptocurrency. But in 2022, they're shaping up to steal even more.

In the first three months of this year, hackers have stolen $1.3 billion from exchanges, platforms, and private entities—and the victims are disproportionately in DeFi.



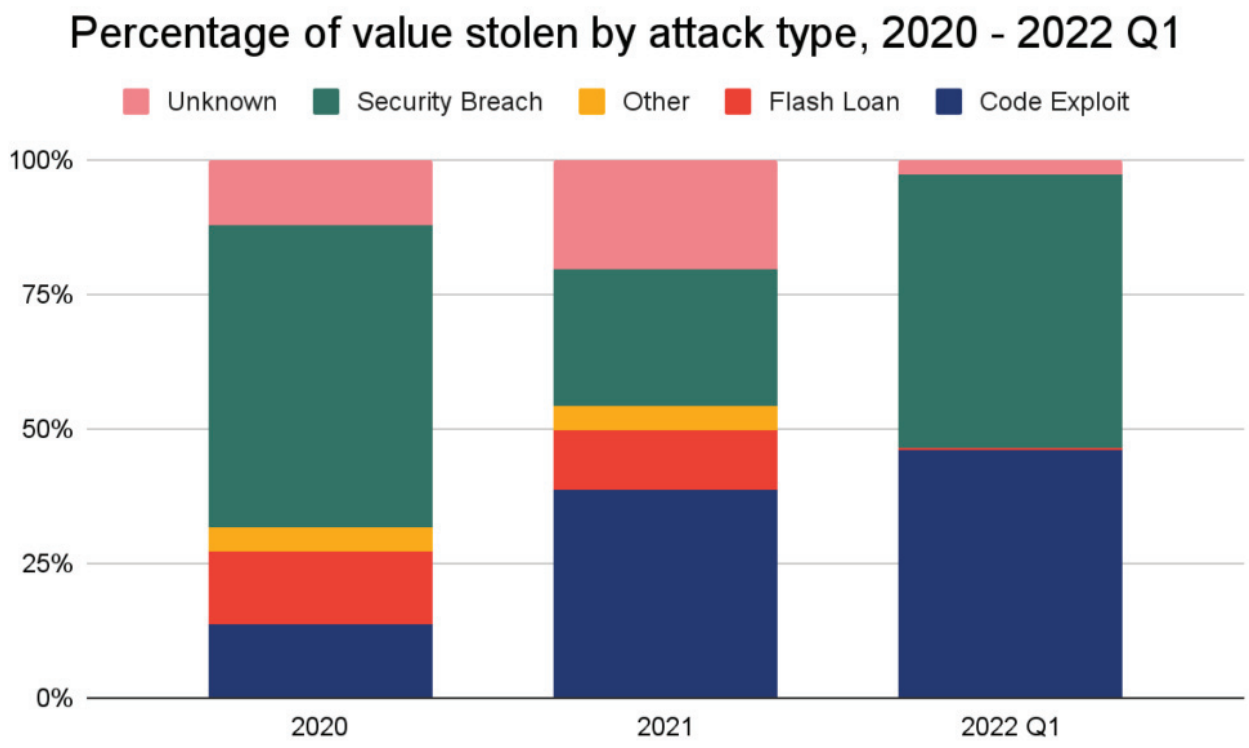
Almost 97% of all cryptocurrency stolen in the first three months of 2022 has been taken from DeFi protocols, up from 72% in 2021 and just 30% in 2020.



Code exploits are an increasingly common vector of attack, but security breaches are here to stay

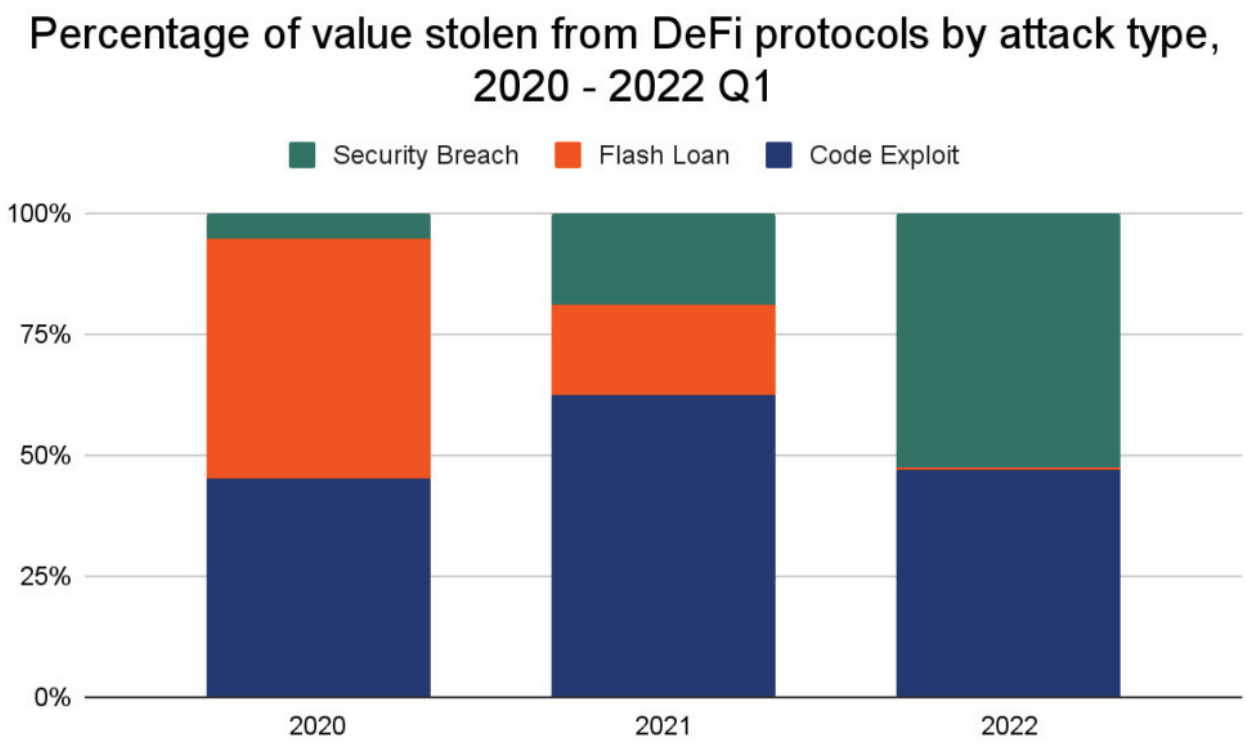
In the past, cryptocurrency hacks were largely the result of security breaches in which hackers gained access to victims' private keys—the crypto-equivalent of pickpocketing. Ronin Network's March 2022 breach, which enabled the theft of $615 million in cryptocurrency, has proven the continued effectiveness of this technique.

Our aggregate data further illustrates this fact. From 2020 to Q1 2022, 35% of all cryptocurrency value was stolen thanks to a security breach.



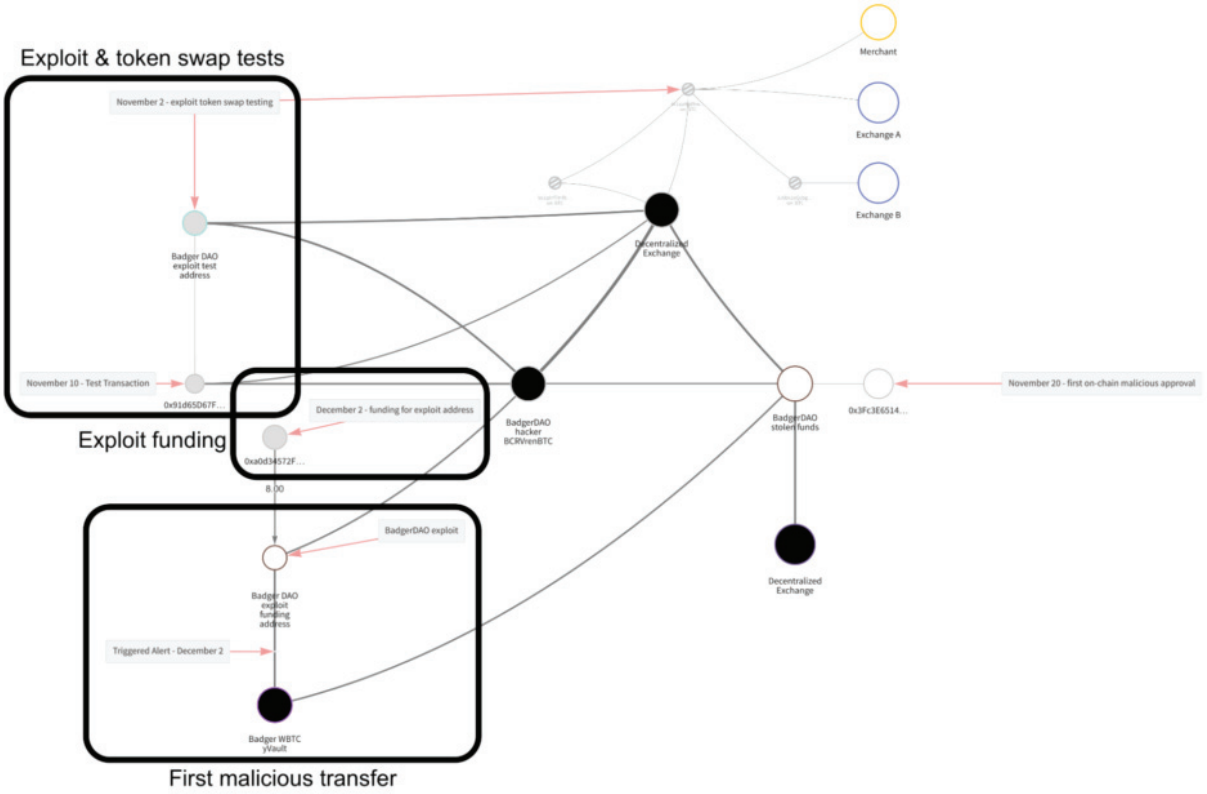
Note: The "unknown" label means information about hack type is not publicly available. The "other" label means the hack type is known but does not fit within our defined categories.

For DeFi protocols in particular, however, the largest thefts are usually thanks to faulty code. Code exploits and flash loan attacks—a type of code exploit involving the manipulation of cryptocurrency prices—has accounted for much of the value stolen outside of the Ronin attack.



Code exploits occur for a number of reasons. For one, in keeping with DeFi's faith in decentralization and transparency, open-source development is a staple of DeFi applications. This is an important and generally positive trend: since DeFi protocols move funds without human intervention, users should be able to audit the underlying code in order to trust the protocol. But this benefits cybercriminals, too, who can analyze the scripts for vulnerabilities and plan exploits well in advance.

In the DeFi hack of BadgerDAO last year, for example, the hacker tested the exploit and laundering process months before the attack.



Flash loan attacks, on the other hand, are sometimes caused by DeFi platforms' reliance on unstable price oracles.

Oracles are tasked with maintaining accurate pricing data for all cryptocurrencies on a platform, and the job isn't easy. Secure but slow oracles are vulnerable to arbitrage; fast but insecure oracles are vulnerable to price manipulation. The latter type often leads to flash loan attacks, which extracted a massive $364 million from DeFi platforms in 2021. In the hack of Cream Finance, for example, a series of flash loans exploiting a vulnerability in the way Cream calculated yUSD's "pricePerShare" variable enabled attackers to inflate yUSD price to double its true value, sell their shares, and make off with $130 million in a single night.

These two dangers—inaccurate price oracles and exploitable code—underscore the need for the security of both. Fortunately, there are solutions. To ensure pricing accuracy, decentralized price oracles like Chainlink can protect platforms against price manipulation attacks. To ensure smart contract security, code audits can steel programs against common hacks like reentrancy, unhandled exceptions, and transaction order dependency.

But code audits aren't infallible. Nearly 30% of code exploits occurred on platforms audited within the past year, as well as a surprising 73% of flash loan attacks. This highlights two potential shortfalls of code audits:

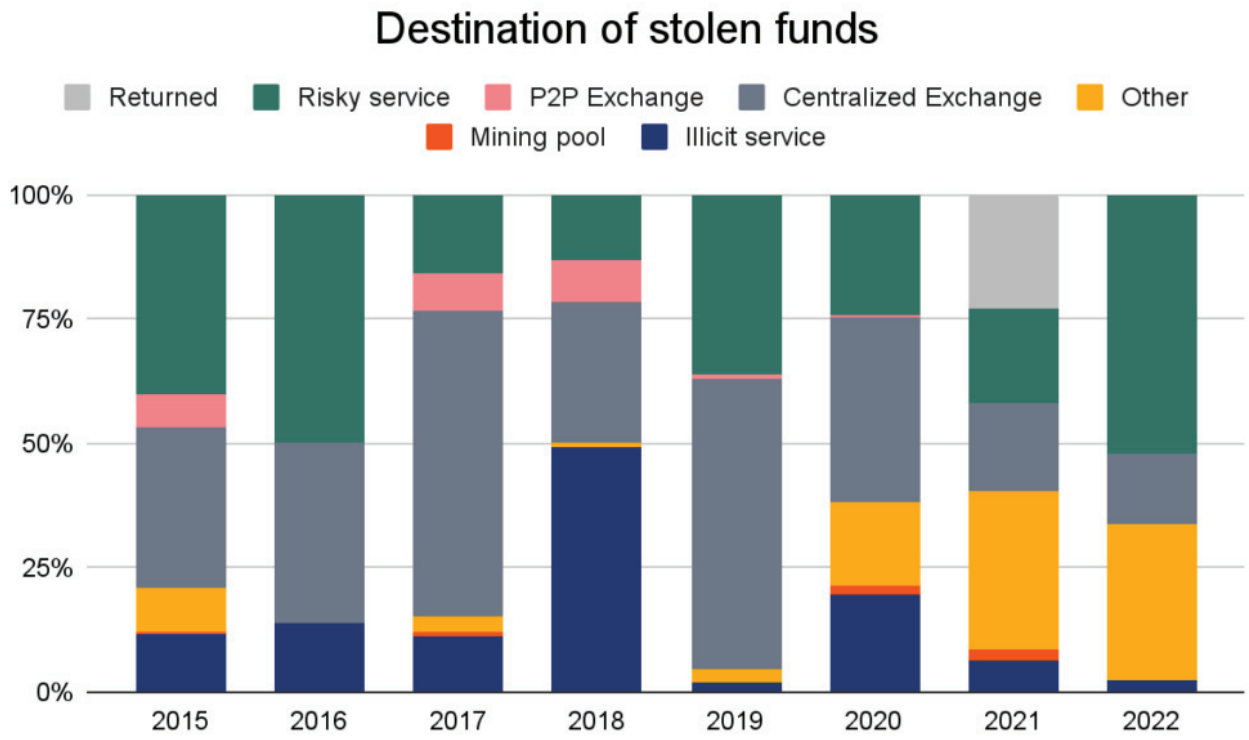
1. They may patch smart contract vulnerabilities *in some cases*, but not all;
2. They seldom guarantee that platforms' price oracles are tamper-proof.

So while code audits can certainly help, DeFi protocols managing millions of users and billions of dollars must adopt a more robust approach to platform security.

Following the money: the final destinations of stolen cryptocurrencies

How do hackers launder stolen cryptocurrency? In 2021, more stolen funds flowed to DeFi platforms (51%) and risky services (25%) than ever before. Centralized exchanges, formerly a top destination for stolen funds, fell out of favor, receiving less than 15% of the total. This is likely due to exchanges' embrace of AML and KYC processes, which threaten the anonymity of cybercriminals.

We've created a new category this year to reflect what may be a first in DeFi hacks we've observed: **returns**. In August of last year, the thief behind the $600 million dollar Poly Network hack returned all $613 million of the funds they stole, and refused the bug bounty they were offered.

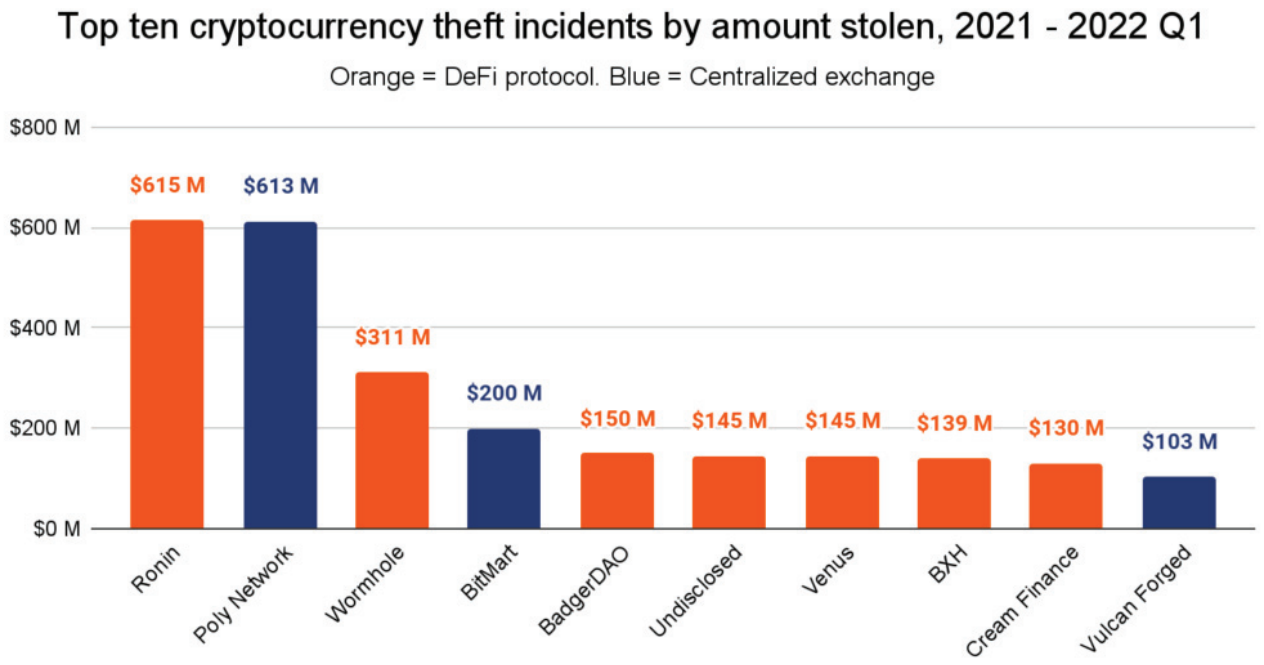


Note: "Risky service" refers to services like mixers, high-risk exchanges, and services based in high-risk jurisdictions.

Not reflected in the graph above is the law enforcement seizure of $3.6 billion worth of cryptocurrency stolen from Bitfinex in 2016. In February 2022, U.S. authorities arrested two individuals who allegedly helped launder the funds taken from Bitfinex during the hack and

were able to recover the majority of the total stolen. This is a very positive development for cryptocurrency users, but it remains to be seen whether this seizure will prompt hackers to change their money laundering strategies moving forward.

The biggest cryptocurrency thefts of 2021 & 2022 Q1



Seven of the ten largest attacks over the past fifteen months have targeted DeFi platforms in particular. These seven DeFi hacks have led to the theft of $1.6 billion, while the three exchange hacks have led to the theft of $960 million.

The following table breaks down the details of each theft.

The Ten Largest Cryptocurrency Thefts of 2021 & 2022 Q1

Victim	Amount stolen (USD)	Service Type	Hack Type	Description
Ronin Network	$615 million	DeFi platform	Security breach	An attacker gained access to five of the nine transaction validators' private keys, then used that majority to sign off ETH and USDC withdrawals.

Poly Network	$613 million	DeFi platform	Code exploit	An attacker exploited cross-chain relay contracts to extract Poly Network's funds on three different chains: Ethereum, BSC, and Polygon. The attacker ultimately returned the stolen funds. Read our complete case study.
Wormhole	$322 million	DeFi platform	Code exploit	An attacker manipulated Wormhole's Solana<->Ethereum cross-chain bridge into believing that 120,000 ETH had been deposited, allowing them to mint whETH (Wormhole ETH) of equivalent value on Solana.
BitMart	$200 million	Exchange	Security Breach	An attacker stole a private key that compromised two of BitMart's hot wallets.
BadgerDAO	$150 million	DeFi platform	Security Breach	An attacker used a compromised cloudflare API key to periodically inject malicious scripts into Badger's application. The scripts intercepted transactions and prompted users to allow a foreign account to operate on their ERC-20 tokens. Once approved, the attacker siphoned funds from the user's wallets.
Undisclosed	$145 million	Private	Other — Embezzlement	An employee allegedly diverted funds to a personal account when the company attempted to transfer funds between financial accounts.
Venus	$145 million	DeFi platform	Code Exploit	An attacker manipulated the price of XVS, the Venus Protocol's governance token, to borrow values of BTC and ETH in excess of XVS's actual value. When the governance token's price declined and protocol users defaulted on their loans, Venus was left with a debt of $145 million.
BXH	$139 million	DeFi platform	Other — Leaked Private Keys	An unidentified member of BXH's technical team allegedly leaked an administrator's private key.

Cream Finance	$130 million	DeFi platform	Flash Loan	An attacker initiated a series of flash loans to mint ~$1.5M of crYUSD. Then, the attacker took advantage of Cream's PriceOracleProxy function to artificially inflate the value of its crYUSD to ~$3B. $2B of this was withdrawn in order to repay the attacker's outstanding flash loans, while the remaining $1B was used to drain all of Cream's assets available for lending ($130M).
Vulcan Forged	$103 million	DeFi platform	Security Breach	An attacker gained access to the private keys of 96 addresses and sent their contents to hacker-controlled wallets.

A cautionary tale for smart contract developers

As the total value locked in DeFi climbs to ever-greater all-time highs — $256 billion at last peak — so too does the risk of exploitation. If there's one takeaway from the meteoric rise in thefts from DeFi platforms, it's the need for smart contract security and price oracle accuracy. Code audits, decentralized oracle providers, and an altogether more rigorous approach to platform security could be the ideal means to that end.

Fortunately, even when these functions do fail and cryptocurrencies are stolen, blockchain analysis can help. Investigators with a full picture of the movement of funds from address to address can take advantage of opportunities to freeze or even seize assets in transit, stopping bad actors before they cash out.

This blog builds on research featured in the 2022 Crypto Crime Report. Download your copy today.